

Declassified in Part - Sanitized Copy Approved for Release 2011/11/10 : CIA-RDP87T00623R000100070029-9

Page Denied

Next 1 Page(s) In Document Denied

2 August 1983

The Honorable Donald J. Devine
Director
Office of Personnel Management
1900 E Street, N. W.
Washington, D. C. 20415

Dear Don,

Enclosed is that portion of the report going to the NSC on countermeasures against the hostile intelligence threat which deals with personnel security programs. Under NSDD-84 the Attorney General has the committee for dealing with personnel security standards. I recommended to Bill Clark that whatever action is taken on this be considered in the light of the recommendations you briefed me on recently so that investigations for security purposes and for suitability purposes are integrated with the view to getting maximum overall effectiveness focused on those levels where the risks are greatest.

Yours,

Bill
William J. Casey

Enclosure

SECRET

CL BY
DECL

DCI
OADR

Distribution:

Orig - Adse
1 - DCI
1 - DDCI
1 - EXDIR
① - D/ICS
1 - DDA
1 - ER



A. Personnel Security Programs

The programs covered under this section include the measures taken to ensure that persons employed by the United States, whether in a civilian or military capacity, or under contract to the United States can be trusted (1) to protect classified information to which they are given access or (2) to undertake responsibilities of sensitive national security duties. The fundamental elements of such programs include:

- o Basic standards upon which personnel security clearance determinations are based.
- o Criteria relating to whether the standard has been met.
- o Background investigations to develop information relevant to the criteria and standard.
- o Adjudication of all relevant background information for the purpose of determining whether the standard has been met.
- o Administrative process to be followed when adverse determinations are made.
- o Continuing security programs, including reinvestigations, designed to detect substantive changes in a cleared individual's security eligibility. [redacted]

25X1

Authority

- There is no law and no single Executive branch policy¹ that specifically authorizes and encompasses all of personnel security. Authority to institute such programs has been implied, however, from the authorities of department and agency heads to manage and operate their respective agencies. Also, the DCI is charged by Executive Order to ensure the establishment by the Intelligence Community of common security and access standards and to protect intelligence sources and methods.

25X1

[redacted] ^{by statute}
There are four relevant Executive Orders. E.O. 10450, entitled "Security Requirements for Federal Employment" issued 27 April 1953,

¹NSDD-84, signed by President Reagan on 11 March 1983, calls for an in-depth review and revision of personnel security policy by the Justice Department, in coordination with OPM, but to date no overall policy in this area exists. [redacted]

25X1

25X1

provides requirements governing the suitability of civilian applicants for Federal employment, which include minimal requirements for persons going into "sensitive" positions. These are positions which, if misused, could bring about, by virtue of the nature of the position, a material adverse effect on the national security. []

25X1

The clearance standard under E.O. 10450 is whether the employment and retention in employment of any civilian officer or employee within a department or agency is "clearly consistent with the interests of the national security". E.O. 10450 charges the head of each department or agency of the Federal Government with "the responsibility for establishing and maintaining within his department or agency an effective program" to insure employees meet the standard. The Office of Personnel Management, as successor to the Civil Service Commission, is given the responsibility "with the continuing advice and collaboration of representatives of the departments and agencies" to make a continuing study of the manner by which E.O. 10450 is being implemented. []

25X1

The second, E.O. 10865, entitled "Safeguarding Classified Information Within Industry" issued 20 February 1960, establishes the standard and procedures for granting contractor employees clearance for access to classified information and provides procedures to appeal proposed adverse actions taken on the basis derogatory information indicating that the standard has not been met. The clearance standard under EO 10865 is that "access to classified information shall be granted or continued only to those applicants who have been determined eligible based upon a finding that to do so is clearly consistent with the national interest." The Department of Defense administers the personnel security aspects of the industrial security program for most departments and agencies of the Federal Government under a standardized approach set forth in the Defense Industrial Security Regulation, DoD 5220.22-R. []

25X1

The third of the Orders, E.O. 12356, entitled "National Security Information" issued 2 April 1982, does not deal with personnel security per se, but provides that persons may not be given access to classified information unless they have been determined to be trustworthy and access is necessary for the performance of official duties. Thus, there is a third personnel security standard, i.e. a determination of "trustworthiness" which must be made. []

25X1

The fourth of the Orders, E.O. 12333, entitled "United States Intelligence Activities" dated 4 December 1981, is applicable solely to intelligence matters and makes the DCI responsible to ensure the establishment by the Intelligence Community of common security and access standards for managing and handling foreign intelligence systems, information, and products, and to ensure that programs are developed which protect intelligence sources, methods, and analytical procedures. Thus, the DCI is responsible for the protection of intelligence

25X1

Government-wide and can limit access to intelligence for failure to meet acceptable security standards. The Order also directs senior officials in the Intelligence Community to protect intelligence and intelligence sources and methods from unauthorized disclosure consistent with guidance from the DCI. These responsibilities, limited as they are to intelligence, have broad implications for U.S. security programs Government-wide. []

25X1

While the approach taken by the various departments and agencies is characterized more by commonality than differences, there is, nevertheless, some variation with respect to procedures concerning investigation and adjudication. For example, departments and agencies with large investigative requirements have generally established their own investigative capabilities; for those whose requirements are small, investigations are conducted by OPM or by arrangement with other departments and agencies with investigative capabilities, such as the FBI. The General Accounting Office (GAO) recently contracted with DoD to have the Defense Investigative Service conduct investigations on certain GAO personnel in sensitive positions. There is no department or agency whose employees or contractors require access to classified information that has not instituted some form of investigation as a condition of clearance. []

25X1

There are two categories of classified information--Sensitive Compartmented Information (SCI), dealing with classified information that reveals foreign intelligence sources and methods, and "Restricted Data," involving nuclear information classified pursuant to the Atomic Energy Act of 1954--for which uniform personnel security requirements are imposed over and beyond those adopted on a decentralized basis pursuant to the three Executive orders cited above. In addition, certain special authorities have been established in law, such as PL 88-290, entitled "Personnel Security Procedures in the National Security Agency," which details the requirement for background investigations for NSA employees. It directs the Secretary of Defense to prescribe such regulations relating to continuing security procedures as he considers necessary to assure that no person is assigned duties in NSA unless such assignment is clearly consistent with the national security. []

25X1

With respect to SCI, the Director of Central Intelligence derives authority under the National Security Act of 1947 to protect intelligence sources and methods and from the provision of Executive Order 12356 that provides for the creation of special access programs by the DCI for intelligence activities or intelligence sources or methods. To carry out this responsibility and to facilitate the security certification process among Government departments and agencies, he has imposed through DCI Directive 1/14 of September 1981 minimum uniform standards on all departments and agencies within the Intelligence Community governing the investigative requirements for persons who will have access to SCI, as

25X1

well as the adjudicative standards upon which a determination regarding access will be based. DCID 1/14 prescribes a fourth national personnel security standard which is that the person being granted SCI access "shall be stable, of excellent character and discretion and of unquestioned loyalty to the United States." [redacted]

25X1

With respect to access to "Restricted Data," the Department of Energy provides uniform standards governing the access of persons to such data for all departments and agencies. [redacted]

25X1

Structure

As mentioned, there is no uniform national personnel security policy which integrates the requirements of all the separate programs involving Federal civilian employees (E.O. 10450), contractor employees (E.O. 10865), access to classified information (E.O. 12356), access to Restricted Data (Atomic Energy Act of 1954), and assignment to National Security Agency duties (PL 88-290). Moreover, while there is a structured and standardized approach within each of the individual programs operating under DCID 1/14, E.O. 10865, the Atomic Energy Act of 1954 and PL 88-290, departments and agencies operating programs outside of those specialized authorities (under E.O. 10450, for example) have, as a practical matter, formulated programs tailored to their own perceived needs, which recognize both the sensitivity of the information to which access is being contemplated, the frequency of such access, and the size of the population requiring such clearance. Thus, there is lacking standardization in the so-called "collateral" (non-SCI) programs. Moreover, these "collateral" programs do not attain the depth that is found in certain other programs. [redacted]

25X1

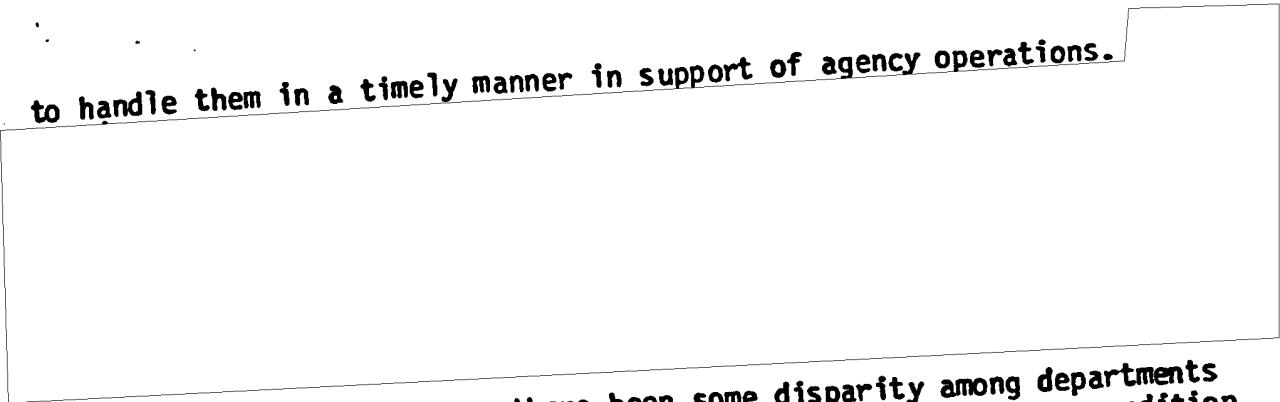
For example, in NSA where all employees are cleared for access and in CIA where all employees are considered approvable for access to sensitive information, more extensive background investigations, polygraph examination, and psychological tests are required of prospective applicants as a condition of employment and for access to any level of classified information. In other agencies where the nature and degree of access to sensitive information varies considerably, such as the Department of Defense (which also has the largest number of cleared civilian, military, and contractor personnel in the Federal Government), State, Treasury, and the various agencies serviced by OPM, lesser requirements for "collateral" clearances are in effect. [redacted]

25X1

Several agencies have also found it necessary from time-to-time to adjust investigative requirements for clearances as a result of increased demands for clearances and the lack of adequate investigative resources

25X1

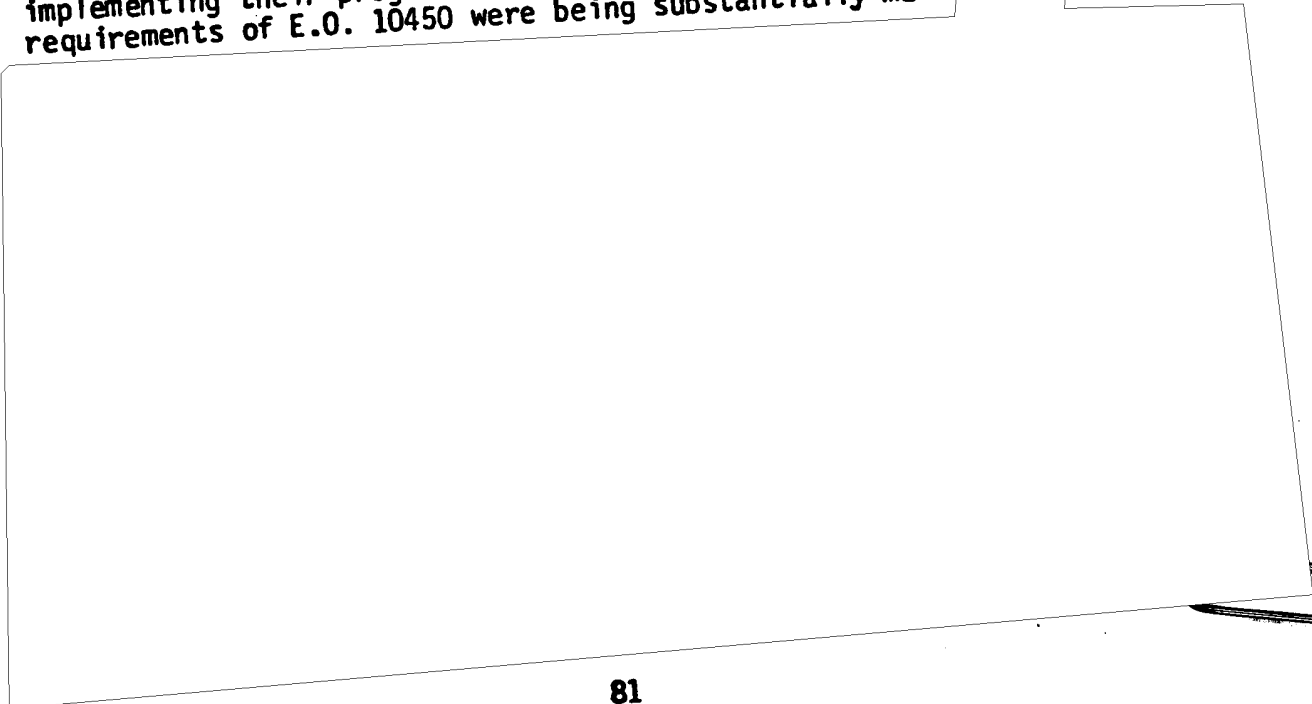
to handle them in a timely manner in support of agency operations.



In short, not only has there been some disparity among departments and agencies in terms of their investigative requirements as a condition of access to classified collateral information, but there has been some fluctuation of such requirements even within agencies due to the ebb and flow of investigative demands and investigative resources.

There is no single department or agency charged with personnel security policy oversight. Clearly, the DCI has oversight responsibility with respect to personnel security in the SCI area. Similarly, the Office of the Secretary of Defense has oversight of the Defense Industrial Security Program covering DoD and 18 other Federal agencies.

 While the OPM, as indicated above, has a limited oversight role under E.O. 10450 with respect to civilian employees, its responsibility does not, nor could it legally, extend to contractor or military personnel. Moreover, even in the area of civilian employees, OPM has traditionally permitted departments and agencies great latitude in implementing their programs so long as it believed the minimal requirements of E.O. 10450 were being substantially met.



Each department or agency is charged with implementing the provisions of DCID 1/14 and for determining the need-to-know of its employees for access to specific compartmented programs. The chart (Figure 5) attached at the end of this section, "Implementation of the SCI Security Clearance Process," illustrates the implementation of the SCI clearance system by the participating agencies. Generally, each agency adjudicates the results of investigations of its own personnel, except for those agencies involved in compartmented programs managed by another agency. SCI accesses granted after adjudication will be recorded centrally

25X1

by CIA as a service of common concern. This system will centralize information presently stored in separate data bases and thus provide Intelligence Community members with the capability to determine the SCI access status of past and present employees. The system began operations in March 1983, with complete implementation in the Intelligence Community expected by early 1984 and in the Unified and Specified Commands by 1984-1985. Similarly, DoD in 1981 initiated a program to have all DoD agencies input all security clearance and access determinations into the Defense Central Index of Investigations, and expects to bring all DoD components into the system in the near future.

25X1

25X1

25X1

Resources

Each department and agency programs and budgets for its own resources to conduct personnel security investigations and carry out related functions, except that DoD carries out all contractor industrial security personnel security investigations and attendant adjudicative processing for 18 other Federal agencies at no cost to these agencies. Most personnel security funding is outside the National Foreign Intelligence Program.

25X1

25X1

Strengths and Weaknesses

The strength of the current personnel security system lies in its flexibility and adaptability to departmental and agency needs. The present system allows the agencies to take into account the type and extent of access, as well as to adjust to changing demands and resource requirements. Cooperation among the departments and agencies in terms of mutual and reciprocal acceptances of clearances and access authorizations of their respective employees has served to facilitate on-going operations. []

25X1

One of the primary weaknesses of the Federal personnel security program is the confusion brought about by E.O. 10450 as the result of its attempting to integrate in a single program "suitability for employment" with "trustworthiness decisions for access to classified information or assignment to national security duties." This has resulted in court decisions that have severely limited the utility of E.O. 10450. Moreover, it has served to cause increasing restrictions being placed on access to criminal history record information in that personnel security checks are considered employment checks. Criminal history record custodians will not provide criminal history records for "employability" determinations, but in most cases will provide such information for national security purposes. In fact, California state law prohibits release of records information for employment reasons. Similarly, the Government of the District of Columbia reaffirmed its restriction against DIS accessing non-conviction arrest information for "employment purposes," basing its decision on the "Duncan Ordinance" which provides that the release of non-conviction arrest information by the Metropolitan Police Department is restricted to law enforcement officers acting in connection with a criminal investigation or criminal proceeding. []

25X1

There is little reason to expect this trend to change unless E.O. 10450 is superseded by an order issued to stress security eligibility vice employability. []

25X1

There is a strong belief among the departments and agencies, particularly those extensively engaged in national security programs, that policy, procedural, and organizational changes may result in a more efficient and effective personnel security program. []

25X1

Considerations for Personnel Security Program Upgrading

1. Perhaps the most significant undertaking under way is the action directed by the President in NSDD-84 by which the Attorney General, on an interagency basis, is to conduct a study of existing related structures, Executive Orders, regulations, and directives for the purpose of identifying ways and means of improving Federal personnel security policies and procedures. The NSDD-84 study

25X1

should include consideration of a new Executive order that would provide specific and exclusive authority for personnel security determinations involving access to classified information and assignment to national security sensitive duties as against suitability for Government employment. The order should include specific national policy pronouncements covering the six basic personnel security elements cited on the opening page of this section. It should provide sufficient flexibility for the various departments and agencies to meet their individual mission requirements while requiring minimum security procedures to assure a sound and effective interrelating national personnel security program. [REDACTED]

25X1

The order should cover Federal civilian employees, Armed Services personnel, and contractor employees in sensitive national security positions. Emphasis should be made in the new order on separating security requirements from the requirements for suitability for Government employment. An interagency mechanism could be established to provide oversight of the new Executive order and to resolve interagency problems, or the Office of Personnel Management could be charged with doing so. [REDACTED]

25X1

The FBI does not favor any standardization process which could mandate a reduction of current FBI clearance standards. It believes that its Director's prerogative to set and execute FBI personnel policies should remain intact. Its concern is that, although limiting the order to only security requirements might meet the standards of certain military/Intelligence Community members, some other members of the Government must rely also on suitability factors. Positions involving trust and responsibility may not optimally allow a separation of suitability from clearance in the order. [REDACTED]

25X1

The majority of the Working Group on Personnel Security convened by the Interagency Group/Countermeasures, on the other hand, believes that an Executive Order separating security determinations from suitability for employment determinations is not only feasible but is essential if the Federal personnel security program is to proceed on an effective basis. [REDACTED]

25X1

2. Greater uniformity in adjudicating security clearances is needed across the Government. Consideration ought to be given to the development of uniform adjudication guidelines to apply to all departments and agencies, as well as centralized training of adjudicators on a periodic basis. In those agencies such as Navy, where the adjudicative function is very widely dispersed (3,000 separate elements), consolidation of this function should be considered to ensure greater consistency in outcome. The FBI would

25X1

oppose any guidelines which would infringe on its Director's role in setting personnel policies within the FBI. DoD would agree to participate in the development of uniform adjudicative guidelines but would consider implementing them only on the condition that they are fully applicable to all Federal departments and agencies.

3. Consideration should be given to the feasibility of establishing a system to facilitate the reallocation(s) of personnel security investigations among departments and agencies at a reasonable cost when conditions within any given agency result in an investigative workload exceeding investigative resources. For example, if DoD, due to the sudden expansion of critical R&D programs, could not complete its required investigations on a timely basis, a means should be available whereby such an agency could request investigative assistance from other agencies at a reasonable cost. The creation of an interagency system where such requests might be brought and deliberated could prevent the development of excessive backlogs during periods of high workload and could additionally obviate the necessity for reduction in force which follows periods of decreased demand for investigations (as recently happened in OPM). CIA cover considerations, however, would not permit its participation in such an arrangement. The FBI could not participate because its investigative resources are already fully committed and it would be unable to absorb any increase. Furthermore, since resource levels are set in budgets several years in advance, it would not be able to accept an influx created by unexpected circumstances. DoD believes that such a system would be unrealistic and unworkable unless all agencies with investigative capability participated, with no agencies being exempted. DoD shares much the same budget and mission considerations as FBI and CIA.

4. Consideration should be given to establishment of a national policy on use of the polygraph as a means of screening for access to classified information, including crypto access and assignment to sensitive national security duties. The CIA would support such a policy but would reserve the right to maintain its own standards separately should they be more stringent than those adopted for Government-wide and industrial contractor use. The FBI would be opposed to any policy which would require it to operate below that which it considers essential or which infringes on its Director's prerogatives in the personnel area.

The DoD would oppose implementing any policy which was not truly a "national" policy. By virtue of the provisions of the National Security Act of 1947 which gives the Secretary of Defense "authority, direction, and control over the Department of Defense"

and which designates the Secretary as the principal assistant to the President in all matters relating to the Department of Defense, DoD would not want to implement any national policy on the use of the polygraph which would give DoD less flexibility and independence than that which would be given to other agencies. [REDACTED]

25X1

The State Department opposes establishment of a general policy requiring its employees to agree to polygraph examinations as a condition of employment or access to classified information. The Department believes that there remain too many legal and personnel-related questions on this issue, and does not believe that the polygraph is a consistently reliable tool for such purposes. The Department has an on-going counterintelligence program that it believes is sufficient for this purpose. [REDACTED]

25X1

5. In light of the diminishing access to criminal history record information across the nation on the part of the personnel security investigative agencies, action should be taken to review existing restrictions on Federal personnel investigative access to state and local agencies, including Federal rules or regulations such as the 1976 Law Enforcement Assistance Agency Regulation. The review should be broad-gauged and cover the scope and nature of the access problems involved. While this has been a particularly difficult problem for the Department of Defense because of the extremely high volume of police record checks required, all agencies are suffering, with the possible exception of the Federal Bureau of Investigation which gains access under its law enforcement role. Moreover, there is a growing trend on the part of states and local criminal history record custodians to charge the Federal Government for making police record checks if the request is for purposes other than law enforcement. If the review's findings deem it necessary, new legislation or a new Executive Order should be proposed to deal with the problems involved. [REDACTED]

25X1

25X1

Page Denied